

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-251714

(43) 公開日 平成9年(1997)9月22日

(51) Int. Cl. ⁴	識別記号	庁内整理番号	F I	特許表示箇所
G 1 1 B 20/10		7736-5D	G 1 1 B 20/10	H
G 0 6 F 1/00	3 7 0		G 0 6 F 1/00	3 7 0 E
G 1 1 B 20/12	1 0 2	9295-5D	G 1 1 B 20/12	1 0 2
H 0 4 N 5/93			H 0 4 N 5/93	E
	7/167			Z
審査請求 未請求 請求項の数9 OL (全15頁)				

(21) 出願番号 特願平8-57800

(22) 出願日 平成8年(1996)3月14日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 原田 俊治

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 弁理士 中島 司朗

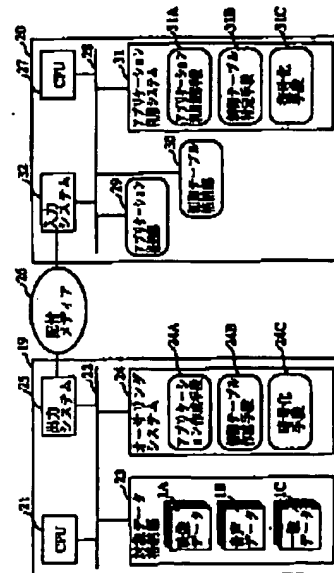
BEST AVAILABLE COPY

(54) 【発明の名称】 ソフトウェア利用制御方式

(57) 【要約】 (修正有)

【課題】 複数のデータを扱うアプリケーションの利用規定を行うに際し、ソフト提供者が、利用制限したり、ユーザの要求に応じて、その制限を解除したり再設定できる。

【解決手段】 アプリケーション作成手段24Aにて、各データもしくはデータの組み合わせ毎に固有の識別子を付与し、制御テーブル作成手段24Bにて、この識別子と各データの利用を制御する情報からなる制御テーブルを2種類作成し、暗号化手段24Cにて、各データと各制御テーブルを暗号化する。ここで第1の制御テーブルには提供者があらかじめ利用を制御するための情報を記述し、第2の制御テーブルには、利用者の要求に応じて変更された利用制御情報を記述可能とする。一方、アプリケーション利用制御手段31Aにて、アプリケーションを利用する際、復号手段31Cにて暗号化された各データと制御テーブルが復号される。



【特許請求の範囲】

【請求項1】複数の対象データを含むアプリケーションにおいて、その利用を制御するソフトウェア利用制御方式において、

アプリケーション提供ステップとアプリケーション利用ステップで構成され、

前記アプリケーション提供ステップは、前記各対象データにそれぞれ固有の識別子を付与する識別子付与ステップと、前記識別子と利用者共通の第1の制御データを構成要素として含む第1の制御テーブルと、前記識別子と利用者個別の第2の制御データを構成要素として含む第2の制御テーブルと、を作成する制御テーブル作成ステップと、前記各対象データと、前記第1の制御テーブルを多重化してアプリケーションを作成する多重化ステップと、前記アプリケーション及び前記第2の制御テーブルを配布する配布ステップと、で構成され、

前記アプリケーション利用ステップは、前記アプリケーションを前記各対象データと前記第1の制御テーブルに分離する分離ステップと、前記第1の制御テーブル及び前記第2の制御テーブルにおける、各対象データに付与された識別子に該当する前記第1の制御データ及び前記第2の制御データを用いて、その対象データの利用を許可するかどうかを判定する利用許可判定ステップと、前記利用許可判定ステップが、許可と判定した場合には前記対象データの利用を可能とし、不許可と判定した場合には前記対象データの利用を不可能とするように対象データの利用を制御する利用制御ステップとで構成されることを特徴とするソフトウェア利用制御方式。

【請求項2】前記多重化ステップは、利用者共通の第1の暗号化ステップによって、多重化されるデータの少なくとも一部を暗号化し、前記分離ステップは、利用者共通の第1の復号化ステップによって、前記暗号化された部分を復号化するようにするか、

または、前記制御テーブル作成ステップは、利用者個別の第2の暗号化ステップによって、前記第2の制御テーブルの少なくとも一部を暗号化し、前記利用許可判定ステップは、利用者個別の第2の復号化ステップによって、前記第2の制御テーブルの暗号化された部分を復号化するようにするか、

の少なくとも一方を施したことを特徴とする請求項1記載のソフトウェア利用制御方式。

【請求項3】前記第1及び第2制御テーブルの少なくとも一方に、各対象データに付与された識別子と、該対象データの利用を可能とするか否かを示す制御データを記載し、前記利用許可判定手段において、前記第1及び第2の制御テーブルに記載された制御データにより、利用の可否を判定するようにするか、

または、前記第1及び第2制御テーブルの少なくとも一方に、各対象データに付与された識別子と、該対象データの利用を許可する利用可能回数、利用可能期間、また

は利用可能時間を示す制御データを記載し、前記利用許可判定手段において、前記第1及び第2の制御テーブルに記載された制御データにより、利用の可否を判定し、利用許可する場合は、利用状況に応じて前記制御データを更新するようにするか、

または、前記第1の制御テーブルに、各対象データ毎に、利用1回単位、利用期間単位、または、利用時間単位の課金料金、またはディスカウント料金を示す制御データを記載し、前記第2の制御テーブルには、利用限度金額を示す制御データを記載しておき、前記利用許可判定手段において、第1の制御テーブルに記載された課金料金が、第2の制御テーブルに記載された利用限度金額以内であれば、利用許可と判定し、前記課金料金やディスカウント料金に応じて利用限度額を更新するようにしたことを特徴とする請求項1、及び2記載のソフトウェア利用制御方式。

【請求項4】前記各対象データが、いくつかのグループに分類される場合に、前記識別子付与ステップは、各対象データに、その対象データが分類される前記グループに固有の識別子を付与するようにするか、

前記識別子付与ステップは、各対象データにそれぞれ固有の第1の識別子を、各グループにそれぞれ固有の第2の識別子を付与し、ここで、各対象データに付与される第1の識別子と、その対象データが分類されるグループに付与される第2の識別子との間に所定の関係を持たせ、前記第1の制御テーブルもしくは第2の制御テーブルには、各グループに固有の第2の識別子と、各グループに分類される各対象データの前記第1の識別子を含め、さらに前記第1の制御テーブルには前記第2の識別子と、前記第1の制御データを、前記第2の制御テーブルは、前記第2の識別子と、前記第2の制御データを、それぞれ含めるようにするか、

のいずれか一方を施したことを特徴とする請求項1及び2記載のソフトウェア利用制御方式。

【請求項5】前記アプリケーションがHPEG方式に基づいて作成される場合に、

前記識別子付与ステップは、各HPEGストリームを識別する識別子を、該HPEGストリームを記述したPES形式のパケットのヘッダ部に記載し、

前記制御テーブル作成ステップは、各HPEGストリームを識別する識別子と、第1の制御データを構成要素とする前記第1の制御テーブルと、各HPEGストリームを識別する識別子と、第2の制御データを構成要素とする前記第2の制御テーブルと、をPES形式のプライベートパケットに記載するようにしたことを特徴とする請求項1、2、3及び4記載のソフトウェア利用制御方式。

【請求項6】前記アプリケーションがHPEG方式に基づいて作成される場合に、

前記第1、および、第2の暗号化ステップは、前記各HPEGストリーム及び前記各制御テーブルを記述しているPE

3

5 形式のパケットのパケットデータ領域を暗号化するようにし、さらに暗号化したことを示す情報を前記PES形式のパケットのスクランブル制御ビット格納領域に記述するようにしたことを特徴とする請求項5載のソフトウェア利用制御方式。

【請求項7】前記アプリケーションがMPEG方式の特にTSストリームに基づいて作成される場合に、

前記第1、および、第2の暗号化ステップは、前記各MPEGストリーム及び前記各制御テーブルを含む各TSパケットのペイロード領域を暗号化するようにし、さらに暗号化したことを示す情報を前記TSパケットのスクランブル制御ビット格納領域に記述するようにしたことを特徴とする請求項5記載のソフトウェア利用制御方式。

【請求項8】複数の対象データを含むアプリケーションの利用を制御するため、当該アプリケーションを含むソフトウェアを製作する方法であって、前記各対象データに固有の識別子を付与する識別子付与ステップと、

全ての利用者に共通した制御データを含む第1の制御テーブルを作成する第1の制御テーブル作成ステップと、個々の利用者からの要求に基づいた各利用者固有の制御データを含む第2の制御テーブルを作成する第2の制御テーブル作成ステップと、

前記各対象データと第1の制御テーブルとを多重化してアプリケーションを作成する多重化ステップと、

全ての利用者を対象として前記アプリケーションを配付する一方、個別の利用者に該当する第2の制御テーブルを配付するステップと、
を備えることを特徴とする利用制御用ソフトウェアの製作方法。

【請求項9】複数の対象データを含むアプリケーションの利用を制御するソフトウェア利用制御方法であって、固有の識別子が付与された各対象データと全ての利用者に共通した制御データを含む第1の制御テーブルとが多重化されたアプリケーションと、個別の利用者に適用されるべき制御データを含む第2の制御テーブルを配信元から受け取るステップと、

受け取ったアプリケーションを各対象データと第1の制御テーブルに分離する分離ステップと、

第1の制御テーブル及び第2の制御テーブルを参照して各対象データの利用が許可されているか否かを判定する判定ステップと、

許可されていると判定した場合には対象データの利用を可能とし、許可されていないと判定した場合には対象データの利用を不可能とするよう対象データの利用を制御する利用制御ステップと、

を備えることを特徴とするソフトウェア利用制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、アプリケーション

4

の利用を制御する方法並びに利用を制御するためのソフトウェアの製作方法に関し、特に複数の動画画や音声などの対象データを含むアプリケーションにおいて、ソフト提供者や利用者の要求に応じて、各対象データ毎や、各対象データの組み合わせ毎に、極めて細かな利用の制御するソフトウェア利用制御方法並びに利用制御用ソフトウェアの製作方法に関する。

【0002】

【従来の技術】従来、複数の動画画、音声、その他一般データを扱うアプリケーションを販売する際、例えば、映画ソフト（映画）の場合では

・映像データと、オリジナルの音声データに、字幕スーパーのデータを付加したソフト

・映像データに、日本語吹替え音声データを付加したソフト

・映像データに、オリジナル音声データと日本語吹替え音声データを付加したソフト

など、同じ映像データに対して、付加される音声データや字幕データの組み合わせによって、様々なバリエーションのソフトをそれぞれ作成し、提供することにより、利用者の様々な要求に応じてきた。

【0003】また、例えば、カラオケソフトの場合でも、歌手別、音楽ジャンル別、年代別など、様々な分類にしたがって多数のカラオケディスクを作成し、販売することにより、ソフト利用者の様々な要求に応じてきた。

【0004】

【発明が解決しようとする課題】しかしながら、従来の映画ソフトの場合では、ソフト提供者にとって、同じ映画ソフトに対して、ソフト利用者の要求に応じるために、ソフトに含める対象データの組み合わせによって、様々なバリエーションのソフトをそれぞれ作成する必要があり、全体の作成コストが大きくなるという問題があった。

【0005】またソフト利用者にとっては、1つのバリエーションを購入した後に、別のバリエーションを利用したい場合、別途購入する必要があり、購入コストが大きくなったり、保管スペースが大きくなるという問題があった。また、カラオケディスクの場合では、ソフト利用者にとっては、自分の好みの曲が、複数のディスクに分散されて収録されている場合、その全てのディスクを購入しなければならなかったり、また、各ディスクに収録された曲が利用者の好みに必ずしも一致しないため、購入コストが割高に感じられるという問題があった。

【0006】これらの問題は、従来のアプリケーション、及び、その再生する装置には、ソフト提供者やソフト利用者の要求に応じて、これらのアプリケーションに含まれる各対象データ毎に、一時的に許可したり、禁止したりするための制御機構がなかったためである。また、このような制御機構を実現する際、ソフトには、従

5

来と異なって利用が許可されていないデータも含まれているので、このようなデータに対する不正利用の問題が新たに生じる。特に、アプリケーションに含まれるデータがデジタル化される場合は、そのままでは、容易にコピーされ、劣化することなく再利用されるという問題もある。

【0007】本発明は、上記従来の問題点に鑑み、第1の目的は、複数の映像データ、音声データ、及び一般データを含むアプリケーションを提供する際に、各データ毎に、ソフト提供者やソフト利用者の要求に応じて、その利用の制御を可能し、提供者の作成コストや、利用者の購入コストを低減できる方式を提供することである。

【0008】第2の目的は、特にアプリケーションに含まれるデータの著作権保護、すなわち、そのデータが、ソフト提供者の意図に反した形で利用されることを防止できる方式を提供することである。第3の目的は、特に有料アプリケーションの多様な販売方法、例えばレンタル期間に応じた課金が可能な方法や、データ毎やデータの利用毎に課金が可能な方式を提供することである。

【0009】第4の目的は、対象データの様々な組み合わせ（グループ）毎に、その利用を制御する際に、利用制御用データのデータ容量を低減した方式を提供することである。第5の目的は、対象データが特にデジタル化されたMPEG仕様のデータである場合に、MPEG仕様に適した方式を提供することである。

【0010】

【課題を解決するための手段】上記目的を達成するために、本発明は、複数の対象データを含むアプリケーションにおいて、その利用を制御するソフトウェア利用制御方式において、アプリケーション提供ステップとアプリケーション利用ステップで構成され、前記アプリケーション提供ステップは、前記各対象データにそれぞれ固有の識別子を付与する識別子付与ステップと、前記識別子と利用者共通の第1の制御データを構成要素として含む第1の制御テーブルと、前記識別子と利用者個別の第2の制御データを構成要素として含む第2の制御テーブルと、を作成する制御テーブル作成ステップと、前記各対象データと、前記第1の制御テーブルを多重化してアプリケーションを作成する多重化ステップと、前記アプリケーション及び前記第2の制御テーブルを配布する配布ステップと、で構成され、前記アプリケーション利用ステップは、前記アプリケーションを前記各対象データと前記第1の制御テーブルに分離する分離ステップと、前記第1の制御テーブル及び前記第2の制御テーブルにおける、各対象データに付与された識別子に該当する前記第1の制御データ及び前記第2の制御データを用いて、その対象データの利用を許可するかどうかを判定する利用許可判定ステップと、前記利用許可判定ステップが、許可と判定した場合には前記対象データの利用を可能とし、不許可と判定した場合には前記対象データの利用を

6

不可能とするように対象データの利用を制御する利用制御ステップとを備えたものである。

【0011】好ましくは、前記多重化ステップは、利用者共通の第1の暗号化ステップによって、多重化されるデータの少なくとも一部を暗号化し、前記分離ステップは、利用者共通の第1の復号化ステップによって、前記暗号化された部分を復号化するようにするか、または、前記制御テーブル作成ステップは、利用者個別の第2の暗号化ステップによって、前記第2の制御テーブルの少なくとも一部を暗号化し、前記利用許可判定ステップは、利用者個別の第2の復号化ステップによって、前記第2の制御テーブルの暗号化された部分を復号化するようにするか、の少なくとも一方を施す。

【0012】好ましくは前記第1及び第2制御テーブルの少なくとも一方に、各対象データに付与された識別子と、該対象データの利用を可能とするか否かを示す制御データを記載し、前記利用許可判定手段において、前記第1及び第2の制御テーブルに記載された制御データにより、利用の可否を判定するようにするか、または、前記第1及び第2制御テーブルの少なくとも一方に、各対象データに付与された識別子と、該対象データの利用を許可する利用可能回数、利用可能期間、または利用可能時間を示す制御データを記載し、前記利用許可判定手段において、前記第1及び第2の制御テーブルに記載された制御データにより、利用の可否を判定し、利用許可する場合は、利用状況に応じて前記制御データを更新するようにするか、または、前記第1の制御テーブルに、各対象データ毎に、利用1回単位、コピー1回単位、利用期間単位、または、利用時間単位の課金料金、またはディスクカウント料金を示す制御データを記載し、前記第2の制御テーブルには、利用限度金額を示す制御データを記載しておき、前記利用許可判定手段において、第1の制御テーブルに記載された課金料金が、第2の制御テーブルに記載された利用限度金額以内であれば、利用許可と判定し、前記課金料金やディスクカウント料金に応じて利用限度額を更新する。

【0013】好ましくは前記各対象データが、いくつかのグループに分類される場合に、前記識別子付与ステップは、各対象データに、その対象データが分類される前記グループに固有の識別子を付与するようにするか、または、前記識別子付与ステップは、各対象データにそれぞれ固有の第1の識別子を、各グループにそれぞれ固有の第2の識別子を付与し、ここで、各対象データに付与される第1の識別子と、その対象データが分類されるグループに付与される第2の識別子との間に所定の関係を持たせ、前記第1の制御テーブルもしくは第2の制御テーブルに、各グループに固有の第2の識別子と、各グループに分類される各対象データの前記第1の識別子を含め、さらに前記第1の制御テーブルには前記第2の識別子と、前記第1の制御データを、前記第2の制御テー

ルは、前記第2の識別子と、前記第2の制御データを、それぞれ含めるようにするか、のいずれか一方を施す。

【0014】好ましくは前記アプリケーションがMPEG方式に基づいて作成される場合に、前記識別子付与ステップは、各MPEGストリームを識別する識別子を、該当MPEGストリームを記述したPES形式のパケットのヘッダ部に記載し、前記制御テーブル作成ステップは、各MPEGストリームを識別する識別子と、第1の制御データを構成要素とする前記第1の制御テーブルと、各MPEGストリームを識別する識別子と、第2の制御データを構成要素とする前記第2の制御テーブルと、をPES形式のプライベートパケットに記載する。

【0015】好ましくは前記アプリケーションがMPEG方式に基づいて作成される場合に、前記第1、および、第2の暗号化ステップは、前記各MPEGストリーム及び前記各制御テーブルを記述しているPES形式のパケットのパケットデータ領域を暗号化するようにし、さらに暗号化したことを示す情報を前記PES形式のパケットのスクランブル制御ビット格納領域に記述する。

【0016】好ましくは前記アプリケーションがMPEG方式の特にTSストリームに基づいて作成される場合に、前記第1、および、第2の暗号化ステップは、前記各MPEGストリーム及び前記各制御テーブルを含む各TSパケットのペイロード領域を暗号化するようにし、さらに暗号化したことを示す情報を前記TSパケットのスクランブル制御ビット格納領域に記述する。

【0017】上記目的を達成するために、本発明は、複数の対象データを含むアプリケーションの利用を制御するため、当該アプリケーションを含むソフトウェアを製作する方法であって、前記各対象データに固有の識別子を付与する識別子付与ステップと、全ての利用者に共通した制御データを含む第1の制御テーブルを作成する第1の制御テーブル作成ステップと、個々の利用者からの要求に基づいた各利用者固有の制御データを含む第2の制御テーブルを作成する第2の制御テーブル作成ステップと、前記各対象データと第1の制御テーブルとを多重化してアプリケーションを作成する多重化ステップと、全ての利用者を対象として前記アプリケーションを配付する一方、個別の利用者に該当する第2の制御テーブルを配付するステップとを備えたものである。

【0018】上記目的を達成するために、本発明は、複数の対象データを含むアプリケーションの利用を制御するソフトウェア利用制御方法であって、固有の識別子が付与された各対象データと全ての利用者に共通した制御データを含む第1の制御テーブルとが多重化されたアプリケーションと、個別の利用者に適用されるべき制御データを含む第2の制御テーブルを配信元から受け取るステップと、受け取ったアプリケーションを各対象データと第1の制御テーブルに分離する分離ステップと、第1の制御テーブル及び第2の制御テーブルを参照して各対

象データの利用が許可されているか否かを判定する判定ステップと、許可されていると判定した場合には対象データの利用を可能とし、許可されていないと判定した場合には対象データの利用を不可能とするよう対象データの利用を制御する利用制御ステップとを備えたものである。

【0019】上記構成により本発明によれば、ソフト提供者は、利用者共通の第1の制御テーブルに、初め状態での利用を制限するための情報を設定し、利用者固有の第2の制御テーブルに、利用者の要求に応じて、その利用制限を変更するための情報を設定することにより、複数の映像データ、音声データ、及び一般データを含むアプリケーションを提供する際に、各データ毎に、ソフト提供者がその利用を制限したり、ソフト利用者の要求に応じて、その制限を解除したり、再設定したりといった、きめ細かな利用制御が可能となる。

【0020】これにより、ソフト提供者にとって、ソフトに含める対象データの組み合わせによって、様々なバリエーションのソフトをそれぞれ作成する必要がなくなり、また、アプリケーションには、各対象データと、利用者共通の第1の制御テーブルは含められるが、利用者個別の第2の制御テーブルは含められないので、アプリケーションの大量生産が可能であり、ソフト提供者の作成コストを低減できる。

【0021】一方ソフト利用者にとっても、1つのバリエーションを購入した後に、別のバリエーションを利用したい場合、別々にソフトを購入する必要がなくなるため、利用者の購入コストを低減できる。また、アプリケーションや制御テーブルは暗号化されるので、その内容が盗み見されたり、改変されたり、流用されるのを防止でき、さらにアプリケーションに含まれるデータの著作権保護、すなわち、そのデータが、ソフト提供者の意図に反した形で利用されるのを防止できる。

【0022】また、2種類の制御テーブルの内容をアプリケーションの販売形態に応じて変えることにより、多様な販売方法、例えばレンタル期間に応じた課金が可能となる方法や、データ毎やデータの利用毎の課金などが可能となる。また、対象データの様々な組み合わせ（グループ）毎に、識別子を付与し、この識別子と制御データを構成要素とする制御テーブルを用いることにより、グループ単位の利用制御を可能とし、さらに制御テーブルのデータ容量を低減できる。

【0023】また、対象データが特にデジタル化されたMPEG仕様のデータである場合に、PES形式のパケットに基づいて制御テーブルを作成し、また暗号化する際には、PES形式もしくはTS形式のパケットのデータ領域を暗号化することにより、MPEG仕様にも適合できる。

【0024】

【発明の実施の形態】以下、本発明を実施例を図面を参照して説明する。

(実施例1) 図1は、本発明に係わるアプリケーション利用制御方式を採用した実施例の概略構成を示すシステム構成図である。また図2は本実施例の全体のデータの流れを説明するための概念図である。

【0025】本実施例では、MPEG(Motion Picture Expert Group)方式に基づいて符号化された映像、音声、及び、その他のデータを含むアプリケーションソフトを、各データ毎に利用制御する例について説明する。

【全体の構成】図1に示すように、本実施例におけるアプリケーション利用制御方式を採用したシステムは、アプリケーションを作成する装置A19と、アプリケーションを利用(再生)する装置B20と、配付メディア26によって構成されている。

【0026】装置Aは、アプリケーション提供者が利用する装置であり、装置A全体の動作を制御するCPU21を有しており、このCPU21は、バス22を介して、

(映像データ1A、音声データ1B、及びその他一般データ1C等からなる)対象データの格納部23と、オーサリングシステム24と、出力システム25とにそれぞれ接続されている。オーサリング24は、対象データを用いてアプリケーションを作成するアプリケーション作成手段24Aと、このアプリケーションの利用を制御するための制御テーブルを作成する制御テーブル作成手段24Bと、必要に応じて、このアプリケーションと制御テーブルを暗号化する暗号化手段24C、が備わっている。

【0027】出力システム25は、作成されたアプリケーションと制御テーブルを配付メディア26へ、この配布メディアに適した形態で出力する。配付メディア26は、アプリケーションと制御テーブルを装置Aから装置Bに配付するためのメディアであり、具体的には、例えば、アプリケーションの配付にはCD-ROMなどが利用でき、また、制御テーブルの配付には、ICカードなどが利用される。

【0028】一方、装置Bは、アプリケーション利用者が利用する装置であり、装置B全体の動作を制御するCPU27を有しており、このCPU27は、バス28を介して、配付メディア26から受け取ったアプリケーションの格納部29と、制御テーブルの格納部30と、アプリケーション利用システム31と、配布メディアからアプリケーションと制御テーブルを受けとる入力システム32に接続されている。

【0029】アプリケーション利用システム31は、暗号化されているアプリケーションと制御テーブルを復号する復号手段31Cと、アプリケーションの利用限定を解除するかどうかを判断する制御テーブル判定手段31Bと、制御テーブル判定手段31Bの判定にしたがって、アプリケーションの利用を制御するアプリケーション利用制御手段31Aとが備わっている。

【全体の動作概略】次に本実施例の全体のデータの流れ

を図2に基づいて説明する。

【0030】なお、以下では簡単のため、暗号化及び復号化処理は省略した場合について説明する。まず、ソフト提供者が、装置Aを制御して映像、音声、及びその他の各種一般データを含むアプリケーションを作成する場合について説明する。ソフト提供者の要求に従った各映像データ1A、各音声データ1B、各一般データ1Cが格納部23から読み出され、オーサリングシステム24内においてそれぞれの符号化手段241A、241B、241C、で符号化された後、識別子付与手段242にて、各データに固有の識別子3が付与される。識別子3の付与された各データを図2中2A、2B、2Cで示す。

【0031】一方、このとき同時に制御テーブル作成手段24Bにて、全利用者共通の第1の制御テーブル5が作成され、ソフト利用者からの要求に応じた、利用者固有の第2の制御テーブル6が作成される。尚、この場合、第1の制御テーブル5の作成は必ず必要であるが、第2の制御テーブル6はソフト利用者から要求があった場合にその都度作成するようにすることもできる。

【0032】前記第1の制御テーブル5には、アプリケーションに含まれる各データの識別子3と、全利用者共通した第1の制御データ7が記述される。また、第2の制御テーブル6には、アプリケーションに含まれる各データの識別子3と、個々の利用者毎に異なる第2の制御データ8が記述される。そして、アプリケーション作成手段24A内において前記識別子3が付与された映像データ2A、音声データ2B、一般データ2Cと第1の制御テーブル5とが多重化されてアプリケーションが作成される。図2中の多重化手段243Aはアプリケーション作成手段24A内の一機能を示している。

【0033】上記の如くして作成されたアプリケーションと第2の制御テーブル6は、それぞれ配付メディア26A、26Bにて利用者に配付される。第1の制御テーブル5と第2の制御テーブル6の一例を図11、及び図13に示す。図11は、映像データ1Aとして3種類(映像1、2、3)、音声データ1Bとして3種類(音声1、2、3)を含むアプリケーションに対して、ソフト提供者が、初期状態では、映像1及び音声1を利用可能とする場合を示している。

【0034】この第1の制御テーブル5中の識別子3は、識別子付与手段242が各映像データ1A、音声データ1B、一般データ1Cに付与する識別子と同一である。即ち、第1の制御テーブルにおいて映像1に付与された識別子"11100001"は識別子付与手段242においても映像1に相当する映像データに付与される。

【0035】また、識別子は計8ビットで構成され、上位ビットでデータの種類(映像、音声、一般データの別)を示し、下位4ビットで同一種類のデータにおける

タイトルの異なったものを示している。そして、映像1と音声1が同一シーン又は同一映画というように同時に再生されるべき関係がある場合は、両者に付した識別子は特定ビット（図示例では6ビット用）を除き同一となるようにしてある。尚、この識別子は対象データ格納部23の格納内容を管理している図示しない管理部において発行される。

【0036】次に図13は第2の制御テーブルで、初期状態では、利用を許可されなかった、映像2及び音声2を、ソフト提供者が利用者の要求により、利用可能とする場合を示す。映像2、音声2の制御データが“1”になっていることがそのことを意味している。この第2の制御テーブルはアプリケーション作成に先立って利用者から要求された情報18に基づいて作成される。

【0037】このように、第1の制御テーブルと第2の制御テーブルを用いることにより、ソフト提供者は、提供するアプリケーションの初期状態における利用を制限したり、利用者の要求に応じて、その制限を解除したり、再設定することができるようになる。次に、ソフト利用者が、装置Bを制御してアプリケーションを利用する場合について説明する。

【0038】配布メディア26、入力システム32を通じて装置Bに入力されたアプリケーション及び第2の制御テーブルは夫々の格納部29、30に格納され、続いてアプリケーション利用システム31内の分離手段311（図2参照）にて、装置Aの多重化と逆の処理を行って、アプリケーション格納部29内のアプリケーションを映像データ2A、音声データ2B、一般データ2C等のデータと第1の制御テーブル5とに分離する。

【0039】そして、制御テーブル判定手段31B内の利用許可判定部15にて、まず第2の制御テーブル14の有無が確認され、第2の制御テーブルが無い場合は、第1の制御テーブルの内容が解釈され、第2の制御テーブルが有る場合は、第1の制御テーブルと、第2の制御テーブルの内容がそれぞれ解釈され、いずれの場合もその内容解釈の結果、該当データの利用を許可する場合に

は許可情報16Aを、許可しない場合には不許可情報16Bをアプリケーション利用制御手段31Aに伝える。

【0040】アプリケーション利用制御手段31Aは、許可情報16Aが通知された場合は、該当データを利用し、不許可情報16Bが通知された場合は、該当データの利用を中止する。利用が許可されると、各データは逆符号化され312A～C、各データ1A～1Cとして出力される。利用許可不許可の一例として、第1、及び第2の制御テーブルが、それぞれ図11、及び図13に示す内容である場合について説明すると、まず初期状態

（すなわち第2の制御テーブルがない場合）では、映像1及び音声1の各データの利用に関しては、利用可能であるが、それ以外は利用不可能と解釈される。一方、制御テーブル2がある場合は、映像1、2及び音声1、2

の各データの利用に関しては、利用可能であるが、映像3、音声3の各データの利用に関しては、利用不可能と解釈される。

【0041】図3は、本実施例の全体の処理の流れを示すフローチャートである。この、フローチャートに従って全体の処理の流れを説明する。まず、装置Aにおいて、アプリケーションと、その利用を制御するための制御テーブルの作成処理を行なう（ステップS101）。その後、アプリケーションと制御テーブルの、装置Aから装置Bへの配付処理を行なう（ステップS102）。

【0042】次いで、装置Bにおいて、制御テーブルの内容にしたがってアプリケーションの利用制御処理を行なう（ステップS103）。装置Aにおける、アプリケーションと第2の制御テーブルの作成処理（前記S101）。図4は、装置Aにおけるアプリケーションと制御テーブルの作成処理を示すフローチャートである。

【0043】アプリケーションと制御テーブルの作成処理は、同図に示すように、ソフト提供者から、アプリケーションと、第2の制御テーブルのいずれを作成するか

の指示を受けとり（ステップS201）、アプリケーションの作成が指示された場合には（ステップS202）、アプリケーション作成処理を行ない（ステップS203）、第2の制御テーブル作成が指示された場合（ステップS204）には、第2の制御テーブル作成処理を行なう（ステップS205）。

【0044】そして、アプリケーション及び第2の制御テーブルは、それぞれ配布メディアに適した形に変換されて出力される（ステップS206）。ここでステップS206において、例えば、アプリケーション配布メディアとしてCD-ROMが利用される場合には、CD-ROMの発行処理（すなわちオーサリングシステムで作成されたアプリケーションに対するマスタリング処理とプレス処理）が行なわれる。一方、第2の制御テーブルの配布メディアとしてICカードが利用される場合には、ICカード書き込み処理が行なわれる。

【0045】次に、図5、図6は、それぞれ、装置Aにおけるアプリケーション作成処理（前記ステップS203）の流れと、第2の制御テーブル作成処理（前記ステップS205）の流れを示すフローチャートである。アプリケーション作成処理（前記ステップS203）は、図5に示すように、まず、映像、音声、その他のデータが、MPEG仕様に基づいて符号化されているMPEGストリームを受けとり（ステップS301）。そして各MPEGストリームに、それぞれ固有の識別子を付与する（ステップS302）。以上の処理が、アプリケーションに含められる全てのMPEGデータに対して実行された後（ステップS303）、ソフト提供者が初期状態でアプリケーション利用を一部許可したい場合（ステップS304）には、第1の制御テーブルを作成する（ステップS305）。そして、識別子の付与された各MPEGデータと、第

1の制御テーブルが多重化されて1つのアプリケーションが作成される(ステップS306)。

【0046】ここで、ステップS301、S302、S303は、通常のMPEG仕様によるアプリケーション作成時に実施される基本的な処理である。しかし、ステップS303からS306は、本実施例におけるアプリケーションの作成に特に必要となる処理である。上記ステップS302で作成されるMPEGストリームの一例を図14に示す。図14は、MPEGストリームが、MPEG仕様で規定されたPES(packetized Elementary Stream)形式に従う場合である。図14における、ストリームID部に各MPEGストリームの識別子を記載する。ただし、MPEGの規定では、このストリームID部には、映像で16種類、音声で32種類しか識別できないので、それ以上の種類のデータを含むアプリケーションに対応するために、PESヘッダの拡張データ部分に、拡張ストリームID部を設け、ここにも記載するようにする。

【0047】なお、MPEGデータの構造及びその詳細な定義については、例えばアスキー出版局「最新MPEG教科書」に詳しい解説がある。上記ステップS305で作成される第1の制御テーブルの一例を図10に示す。図10は第1の制御テーブルが、MPEG仕様で規定されたPES形式のプライベートパケットに従う場合である。図10に示すように、パケットデータ領域の先頭には、本実施例で利用する制御テーブルであることを識別する識別コードや、テーブル種別(第1の制御テーブルか、第2の制御テーブルかを区別するデータ)などを記載する。図10では、テーブル種別が0であれば、第1の制御テーブルであることを示している。そして、その後の領域に、各データ毎に、その識別子と、該当MPEGストリームの利用を可とするか/不可とするかを示す制御データを繰り返し記載する。

【0048】図11に、第1の制御テーブルの内容の例を示す。図11については既に説明したので、説明は省略する。次に、上記ステップ306で作成されるアプリケーションについてであるが、MPEGでは、多重化してアプリケーションを作成する際、PS(program stream)形式と、TS(transport stream)形式の2種類のデータ構造を規定していて、このいずれを用いるかは、アプリケーションに依存する。例えば、ディジタル衛星放送では、TS形式を用いるのが一般的であるが、DVD(ディジタルビデオディスク)ではPS形式を用いるのが一般的である。そして、上記PES形式のパケットは、PS形式、TS形式で共用できるようにデータ構造が規定されており、PS形式で多重化することも、TS形式で多重化することも可能である。

【0049】次に第2の制御テーブル作成処理は、図8に示すように、ソフト利用者からの要求情報を受けとる(ステップS401)。そして、その要求情報にしたがって、第2の制御テーブルを作成する(ステップS40

2)。上記ステップS402で作成される第2の制御テーブルの一例を図12に示す。図12は第2の制御テーブルが、PES形式のプライベートパケットに従う場合である。図12に示すように、パケットデータ領域の先頭には、本実施例で利用する制御テーブルであることを識別する識別コードや、テーブル種別(第1の制御テーブルか、第2の制御テーブルかを区別するデータ)などを記載する。図12では、テーブル種別が1であれば、第2の制御テーブルであることを示している。そして、その後の領域に、各データ毎に、その識別子と、該当MPEGストリームの利用を可とするか/不可とするかを示す制御データを繰り返し記載する。図13に、第2の制御テーブルの内容の例を示す。図13については既に説明したので、ここでの説明は省略する。

【0050】図7は、装置Bにおけるアプリケーション利用制御処理の流れを示すフローチャートである。アプリケーション利用制御処理は、図7に示すように、利用するアプリケーションと、第2の制御テーブルが有る場合は、第2の制御テーブルを受けとる(ステップS501)。そして、アプリケーション利用システム31にて、各MPEGデータが利用される際に、第2の制御テーブルの有無が確認され(ステップS502)、第2の制御テーブルが有る場合は、アプリケーションに多重化されている第1の制御テーブルと、この第2の制御テーブルに基づくアプリケーションの利用処理を行ない(ステップS503)、第2の制御テーブルが無い場合は、アプリケーションに多重化されている第1の制御テーブルのみに基づくアプリケーションの利用処理を行ないアプリケーションの利用処理を行なう(ステップS504)。

【0051】ここで、ステップS501において、例えば、アプリケーション配布メディアとしてCD-ROMが利用される場合には、CD-ROM読み込み処理が行なわれる。また第2の制御テーブル配布メディアとしてICカードが利用される場合には、ICカード読み込み処理が行なわれる。図8、図9はそれぞれ、第1の制御テーブルのみに基づくアプリケーションの利用処理と、第1、第2の制御テーブルに基づくアプリケーションの利用処理の流れを示すフローチャートである。

【0052】図8に示すように、第1の制御テーブルのみに基づくアプリケーションの利用処理は、多重化されたアプリケーションが分離され、各MPEGストリームと第1の制御テーブルに分離される(ステップS601)。そして各データを利用する際に、この第1の制御テーブルの内容が解釈される(ステップS602a、b)。すなわち、この第1の制御テーブルの中の、利用するデータに付与された識別子に該当する第1の制御データを参照する。そして、この第1の制御データが、利用許可を示す場合には、該当MPEGストリームを利用(再生)する(ステップS603)。一方、この第1の制御データが

利用不可を示す場合には該当MPEGストリームの利用（再生）は中止する。

【0053】この処理を、各MPEGストリームの再生が終了するまで繰り返す（ステップS604）。一方、図9に示すように、第1、第2の制御テーブルに基づくアプリケーションの利用処理は、まず、多重化されたアプリケーションが分離され、各MPEGストリームと第1の制御テーブルに分離される（ステップS701）。そして各データを利用する際に、この第1の制御テーブルと、第2の制御テーブルの内容が解釈される（ステップS702a、b）。

【0054】具体的には、例えば、第1の制御テーブルの中の利用するデータに付与された識別子に該当する第1の制御データが利用不可を示している、第2制御テーブルの中の、利用するデータに付与された識別子に該当する第2の制御データが、利用許可を示す場合には、該当MPEGストリームを利用（再生）する（ステップS603）。一方、この第2の制御データが利用不可を示す場合には、該当MPEGストリームの利用（再生）は中止する。

【0055】この処理を、各MPEGストリームの利用（再生）が終了するまで繰り返す（ステップS704）。以上の構成により、複数の映像データ、音声データ、及び一般データを含むアプリケーションを提供する際に、各データ毎に、ソフト提供者がその利用を制限したり、ソフト利用者の要求に応じて、その制限を解除したり、再設定したりといった、きめ細かな利用制御が可能となるという効果が得られる。

【0056】また、ソフト提供者にとって、ソフトに含める対象データの組み合わせによって、様々なバリエーションのソフトをそれぞれ作成する必要がなくなり、また、アプリケーションには、各対象データと、利用者共通の第1の制御テーブルは含められるが、利用者個別の第2の制御テーブルは含められないので、アプリケーションの大量生産が可能であり、ソフト提供者の作成コストを低減できる。一方ソフト利用者にとっても、1つのバリエーションを購入した後に、別のバリエーションを利用したい場合、別々にソフトを購入する必要がなくなるため、利用者の購入コストを低減できる。

【0057】また、対象データが特にMPEG方式仕様のデータである場合に、MPEG仕様に適合させることができるという効果が得られる。なお、本発明は、以上説明した実施例に限定されず種々の変形が可能である。その例としては例えば次のものがある。

(A) 本実施例では、暗号化についての記述は省略したが、アプリケーションを多重化する際、アプリケーションを暗号化し、また制御テーブルを作成する際、制御テーブルを暗号化するという態様での実施が望ましい。

【0058】この場合、アプリケーションを分離するに際し、及び制御テーブルの内容を判定するに際し、それ

ぞれ暗号化されたアプリケーション及び制御テーブルを復号化する。以下に、暗号化及び復号化を行なう場合の詳細な動作例を示す。まず、暗号化する際に、利用者共通の第1の制御テーブル、及び各対象データを含むアプリケーションは、利用者共通の鍵で暗号化し、利用者個別の第2の制御テーブルは、利用者個別の鍵で暗号化するようにする。そして、復号化する際に、まず各制御テーブルを復号するようにする。すなわち第1の制御テーブルは利用者共通の鍵で復号化し、第2の制御テーブルは利用者個別の鍵で復号化する。そして、第1、及び第2の制御テーブルの内容を解釈し、該当の対象データが利用可能と判定された場合、その対象データを利用者共通の鍵で復号化する。しかし該当の対象データが利用不可能と判定された場合、その対象データの復号化は行なわない。

【0059】このように復号化する際、まず制御テーブルの復号を行ない、次に、データの復号を、制御テーブルの判定の結果、利用可能と判定された後で行なうのが望ましい。この構成では、利用不可と判断されたデータは全く復号されないため、安全性がさらに向上する。以上のような構成により、アプリケーションや制御テーブルは暗号化されるので、その内容が盗み見されたり、改変されたり、流用されるのを防止でき、さらにアプリケーションに含まれるデータの著作権保護、すなわち、そのデータが、ソフト提供者の意図に反した形で利用されるのを防止できるという効果が得られる。

【0060】なお、上記例では、第2の制御テーブルと、アプリケーションの両者を暗号化したが、いずれか一方のみを暗号化する構成も可能である。例えば、第2の制御テーブルの配布メディアとしてICカードが利用される場合には、配布内容が盗み見されたり、改変されたり、流用される恐れは少ない（物理的に安全）なので、第2の制御テーブルは暗号化しない構成も可能である。

【0061】また、特にアプリケーションがMPEG方式に基づいて作成される場合には、各MPEGストリーム及び各制御テーブルを記述しているPES形式のパケットのパケットデータ領域を暗号化するようにし、さらに暗号化したことを示す情報をPES形式のパケットのスクランブル制御ビット格納領域に記述する構成が可能である。（図10、12、及び14参照）

また特にアプリケーションがMPEG方式のTSストリームに基づいて作成される場合に、各MPEGストリーム及び各制御テーブルを含む各TSパケットのペイロード領域を暗号化するようにし、さらに暗号化したことを示す情報をTSパケットのスクランブル制御ビット格納領域に記述する構成が可能である。（図15参照）

また、暗号化は必ずしも対象データの全体に対して施す必要はなく、暗号・復号処理によるオーバーヘッドと、スクランブル効果との兼ね合いから、アプリケーション毎に最適な暗号化範囲を決定するのが望ましい。

(B) 各制御テーブルに、各データに付与された識別子と、そのデータが利用可能か否かを示す制御データを記述する構成としたが、このような構成に限定されるものではなく、例えば、そのデータが利用可能か否かを示す制御データに変えて、そのデータの利用を許可する限度回数を記述することにより、各データの利用回数を制御することが可能となる。

【0062】また、そのデータが利用可能か否かを示す制御データに変えて、そのデータの利用を許可する期間を記述することにより、各データの利用期間を制御することが可能となる。また、利用者共通の第1の制御テーブルには、各データ毎に各データの利用料金を記述しておき、利用者固有の第2の制御テーブルには、利用者がすでに支払った金額か、または、利用者にあらかじめ許された金額を示す利用限度金額を記述しておき、利用許可判定手段において、第1の制御テーブルに記述された利用料金が、第2の制御テーブルに記述された利用限度金額以内であれば、利用許可を与える一方、利用限度額を更新する構成が可能である。

【0063】これらの構成により、特に有料アプリケーションの多様な販売方法、例えばレンタル期間に応じた課金が可能な方法や、データ毎やデータの利用毎に課金が可能となるという効果が得られる。

(C) 実施例では、各対象データ単位で利用制御する場合について説明したが、様々なデータの組み合わせ単位(グループ単位)で利用制御する構成も可能である。

【0064】例えば、各データに、データ固有の識別子に変えて、分類されるグループに固有の識別子(以下グループ識別子と称する)を付与する構成が可能である。このとき、各制御テーブルには、グループ識別子と、このグループ単位で利用を制御する制御データを記述する。図16にこの構成を採用した場合の第1、第2制御テーブルの例を示す。この例では、映像1と音声1、映像2と音声2、映像3と音声3がそれぞれグループ1、2、3を形成し、グループ1、2及び3には、それぞれ、識別子F1、F2、F3(16進表記)を与える。そして、図示しないが、映像1及び音声1には、識別子(F1)が、映像2と音声2には識別子(F2)が、映像3と音声3には識別子(F3)が付与されている。そして、例えば第1の制御テーブルでは、グループ1は、利用可能であるが、グループ2及びグループ3は、利用不可能であることを示す。

【0065】また、各データに、固有の識別子(以下データ識別子と称する)を付与し、各制御テーブルのいずれか一方に、各グループに固有の識別子(以下グループ識別子と称する)と、データ識別子を記述し、どのグループにはどのデータが含まれるかを判定できるようにし、さらに各制御テーブルには、グループ識別子と、このグループ単位で利用を許可するか否かを示す制御データを記述する構成が可能である。このとき、各データに

付与するデータ識別子を、それぞれ分類されるグループの識別子と識別子関連規定を定め、関連付けを可能にしておく。図17にこの構成を採用した場合の第1、第2の制御テーブルの例を示す。

【0066】この例では、映像1と音声1、映像2と音声2、映像3と音声3が、それぞれグループ1、2、3を形成し、グループ1、2及び3には、それぞれ、グループ識別子F1、F2、F3(16進表記)を与える。さらに、映像1及び音声1にはそれぞれデータ識別子E1、B1、映像2及び音声2にはそれぞれデータ識別子E2、B2、映像3及び音声3にはそれぞれデータ識別子E3、B3を付与する。この例では、識別子関連規定は、グループnにはグループ識別子Fnを与え、グループnに含まれる映像n、及び音声nにはそれぞれデータ識別子En、Bnを与えるという規定を採用している。そして、例えば第1の制御テーブルでは、グループ1は、利用可能であるが、グループ2及びグループ3は、利用不可能であることを示す。

【0067】次に、グループ識別子を採用した場合と、採用していない場合における制御テーブルの容量の比較を、説明に用いた具体例の場合について行なう。まず、グループ識別子を採用した図16の例は、グループ識別子を採用していない図11及び図13の例と同じである。これから明らかにように、テーブル容量は、第1の制御テーブル、第2の制御テーブルとも、図16が図11の半分となる。

【0068】また、グループ識別子を採用した図17の例と、グループ識別子を採用していない図11及び図13の例と同じである。これから明らかにように、テーブル容量は、第1の制御テーブルはほぼ容量であるが、第2の制御テーブルは、図16が図11の半分となる。これらの構成により、対象データの様々な組み合わせ(グループ)毎に、その利用を制御する際に、利用制御用データのデータ容量を低減できるという効果が得られる。

(D) 本実施例では、アプリケーションの配布メディアとして、CD-ROM、限定解除用テーブルの配布メディアとして、ICカードとしたが、その他の配布メディア、例えば、アプリケーション配布メディアとしては、DVD(デジタルビデオディスク)などの記録メディアや、衛星やCATVなどの各種通信網を利用した放送、通信メディアを制御テーブル配布メディアとしては、磁気カードなどを利用することができる。

【0069】また、アプリケーションと制御テーブルを別のメディアで配布するとしたが、同一のメディアを利用しても構わない。なお、配布メディアとして、データの読み書きが比較的簡単な記録メディアや、盗み見、データ採取が容易な通信メディアを利用する際は、配布されるデータを暗号化するのが望ましい。

(E) 本実施例では、1つのアプリケーションが多重化される場合について説明したが、複数のアプリケーション

ンが多重化されてもよい。その場合は、各アプリケーション毎に、制御テーブルがそれぞれ用意され、それら制御テーブルは、各アプリケーション毎に付与された固有の識別子で区別する構成が可能である。

(P) 本実施例では、MPG仕様に基づいたアプリケーションの場合について説明したが、その他の仕様に基づいたアプリケーションに対しても適用可能である。

(G) 本実施例で利用とは人の使用に供するという意味であり、従ってその形態としては試用コピー等を含むものである。

【0070】

【発明の効果】以上の説明から明らかなように、本発明においては、以下の効果が得られる。

(1) 各対象データにそれぞれ固有の識別子を付与する識別子付与ステップと、前記識別子と利用者共通の第1の制御データを構成要素として含む第1の制御テーブルと、前記識別子と利用者個別の第2の制御データを構成要素として含む第2の制御テーブルと、を作成する制御テーブル作成ステップと、前記各対象データと、前記第1の制御テーブルを多重化してアプリケーションを作成する多重化ステップと、前記アプリケーション及び前記第2の制御テーブルを配布する配布ステップと、を備えたアプリケーション提供ステップと、前記アプリケーションを前記各対象データと前記第1の制御テーブルに分離する分離ステップと、前記第1の制御テーブル及び前記第2の制御テーブルにおいて、各対象データに付与された識別子に該当する前記第1の制御データ及び前記第2の制御データを用いて、その対象データの利用を許可するかどうかを判定する利用許可判定ステップと、前記利用許可判定ステップが、許可と判定した場合には前記対象データの利用を可能とし、不許可と判定した場合には前記対象データの利用を不可能とするように対象データの利用を制御する利用制御ステップとを備えたアプリケーション利用ステップと、を備えることにより複数の映像データ、音声データ、及び一般データを含むアプリケーションを提供する際に、各データ毎に、ソフト提供者がその利用を制限したり、ソフト利用者の要求に応じて、その制限を解除したり、再設定したりといった、きめ細かな利用制御を可能とし、提供者の作成コストや、利用者の購入コストを低減できる方式を提供可能となる。

(2) 前記多重化ステップは、利用者共通の第1の暗号化ステップによって、多重化されるデータの少なくとも一部を暗号化し、前記分離ステップは、利用者共通の第1の復号化ステップによって、前記暗号化された部分を復号化するようにするか、または、前記制御テーブル作成ステップは、利用者個別の第2の暗号化ステップによって、前記第2の制御テーブルの少なくとも一部を暗号化し、前記利用許可判定ステップは、利用者個別の第2の復号化ステップによって、前記第2の制御テーブルの

暗号化された部分を復号化するようにするか、の少なくとも一方を施す構成を備えることにより、アプリケーションに含まれるデータの著作権保護、すなわち、そのデータが、ソフト提供者の意図に反した形で利用されることを防止することが可能となるとともに、アプリケーションを様々な媒体で利用者に提供する際に、安全性を高めた方式を提供可能となる。

(3) 前記第1及び第2制御テーブルの少なくとも一方に、各対象データに付与された識別子と、該対象データの利用、試用、またはコピー、を可能とするか否かを示す制御データを記載し、前記利用許可判定手段において、前記第1及び第2の制御テーブルに記載された制御データにより、利用、試用、またはコピーの可否を判定するようにするか、または、前記第1及び第2制御テーブルの少なくとも一方に、各対象データに付与された識別子と、該対象データの利用を許可する利用可能回数、利用可能期間、または利用可能時間を示す制御データを記載し、前記利用許可判定手段において、前記第1及び第2の制御テーブルに記載された制御データにより、利用の可否を判定し、利用許可する場合は、利用状況に応じて前記制御データを更新するようにするか、または、前記第1の制御テーブルに、各対象データ毎に、利用1回単位、コピー1回単位、利用期間単位、または、利用時間単位の課金料金、またはディスカウント料金を示す制御データを記載し、前記第2の制御テーブルには、利用限度金額を示す制御データを記載しておき、前記利用許可判定手段において、第1の制御テーブルに記載された課金料金が、第2の制御テーブルに記載された利用限度金額以内であれば、利用許可と判定し、前記課金料金やディスカウント料金に応じて利用限度額を更新する構成を備えることにより、特に有料アプリケーションの多様な販売方法、例えばレンタル期間に応じた課金が可能な方法や、データ毎やデータの利用毎に課金が可能な方式を提供可能となる。

(4) 前記各対象データが、いくつかのグループに分類される場合に、前記識別子付与ステップは、各対象データに、その対象データが分類される前記グループに固有の識別子を付与するようにするか、または、前記識別子付与ステップは、各対象データにそれぞれ固有の第1の識別子を、各グループにそれぞれ固有の第2の識別子を付与し、ここで、各対象データに付与される第1の識別子と、その対象データが分類されるグループに付与される第2の識別子との間に所定の関係を持たせ、前記第1の制御テーブルもしくは第2の制御テーブルに、各グループに固有の第2の識別子と、各グループに分類される各対象データの第1の識別子を含め、さらに前記第1の制御テーブルには前記第2の識別子と、前記第1の制御データを、前記第2の制御テーブルは、前記第2の識別子と、前記制御データを、それぞれ含めるようにし、前記第1の識別子、前記第2の識別子とするか、の

いずれか一方を施す構成を備えることにより、対象データの様々な組み合わせ（グループ）毎に、その利用を制御する際に、利用制御用データのデータ容量を低減した方式を提供可能である。

（５）前記アプリケーションがMPEG方式に基づいて作成される場合に、前記アプリケーションがMPEG方式に基づいて作成される場合に、前記識別子付与ステップは、各MPEGストリームを識別する識別子を、該当MPEGストリームを記述したPES形式のパケットのヘッダ部に記載し、前記制御テーブル作成ステップは、各MPEGストリームを識別する識別子と、第１の制御データを構成要素とする前記第１の制御テーブルと、各MPEGストリームを識別する識別子と、第２の制御データを構成要素とする前記第２の制御テーブルと、をPES形式のプライベートパケットに記載する構成を備えることにより、また前記アプリケーションがMPEG方式に基づいて作成される場合に、前記第１、および、第２の暗号化ステップは、前記各MPEGストリーム及び前記各制御テーブルを記述しているPES形式のパケットのパケットデータ領域を暗号化するようにし、さらに暗号化したことを示す情報を前記PES形式のパケットのスクランブル制御ビット格納領域に記述する構成を備えることにより、また前記アプリケーションがMPEG方式の特にTSストリームに基づいて作成される場合に、前記第１、および、第２の暗号化ステップは、前記各MPEGストリーム及び前記各制御テーブルを含む各TSパケットのペイロード領域を暗号化するようにし、さらに暗号化したことを示す情報を前記TSパケットのスクランブル制御ビット格納領域に記述する構成を備えることにより、MPEG仕様に適した方式を提供可能となる。

【図面の簡単な説明】

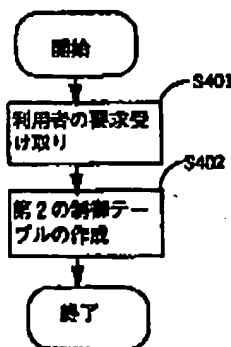
【図１】本発明の実施例におけるソフトウェア利用制御方式のシステム構成図

【図２】実施例における全体のデータの流れ示す概要図

【図３】実施例におけるシステム全体の処理の流れを示すフローチャート

【図４】実施例における装置A全体の処理の流れを示す

【図６】



フローチャート

【図５】実施例におけるアプリケーション作成処理の流れを示すフローチャート

【図６】実施例における限定解除テーブル作成処理の流れを示すフローチャート

【図７】実施例における装置B全体の処理を示すフローチャート

【図８】実施例における利用限定されたアプリケーションの再生処理を示すフローチャート

10 【図９】実施例における限定解除されたアプリケーションの再生処理を示すフローチャート

【図１０】第１の制御テーブルのデータ構造例

【図１１】第１の制御テーブルのデータ例

【図１２】第２の制御テーブルのデータ構造例

【図１３】第２の制御テーブルのデータ例

【図１４】PES形式のパケットのデータ構造例

【図１５】TS形式のパケットのデータ構造例

【図１６】グループ単位で利用制御する場合の各制御テーブルのデータ例１

20 【図１７】グループ単位で利用制御する場合の各制御テーブルのデータ例２

【符号の説明】

10 装置A

20 装置B

21 CPU

22 バス

23 対象データ

24 オーサリングシステム

25 出力システム

30 26 配布メディア

27 CPU

28 バス

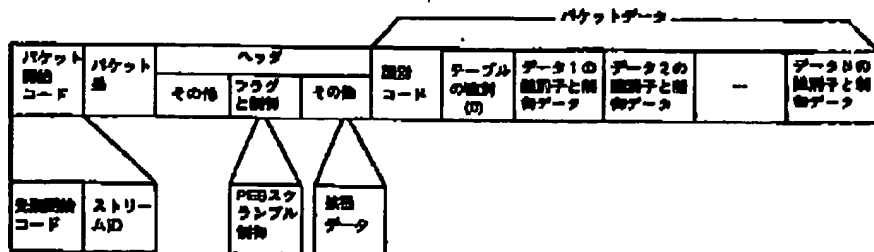
29 アプリケーション

30 制御テーブル

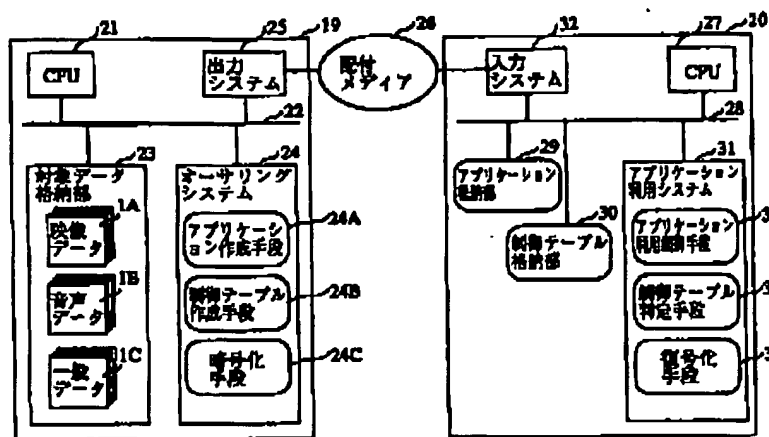
31 アプリケーション利用システム

32 入力システム

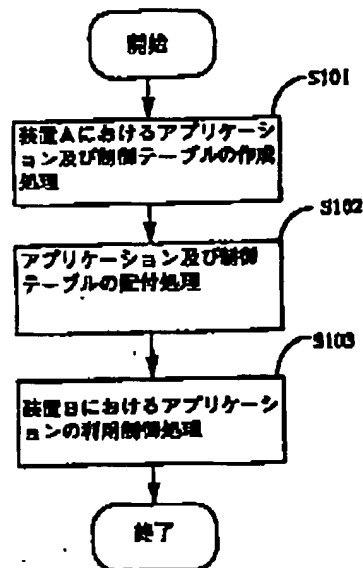
【図１０】



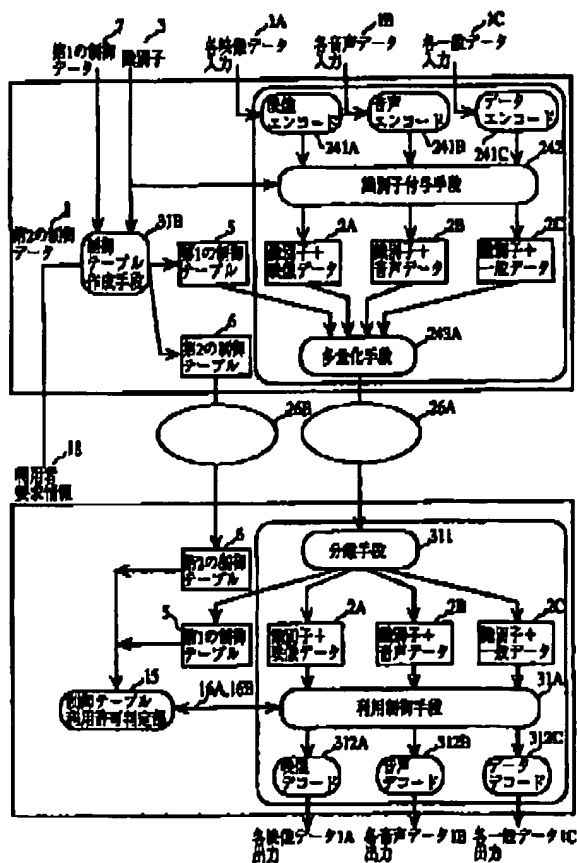
【図1】



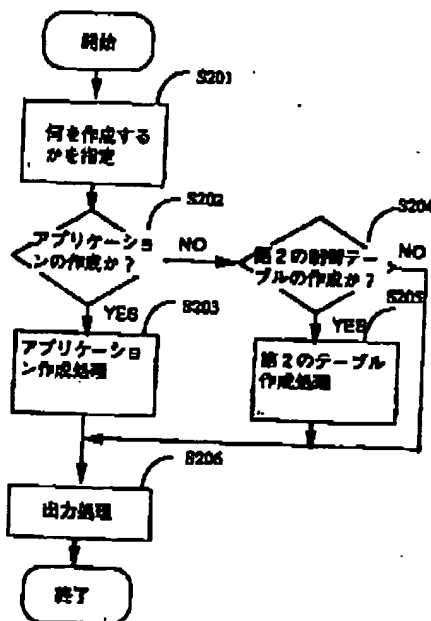
【図3】



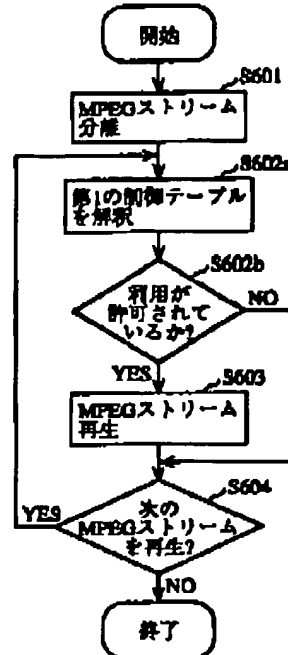
【図2】



【図4】

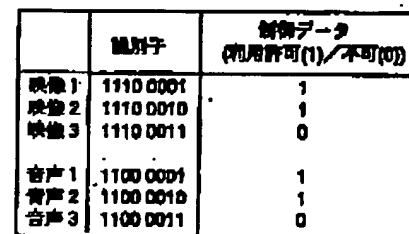


【圖 8】

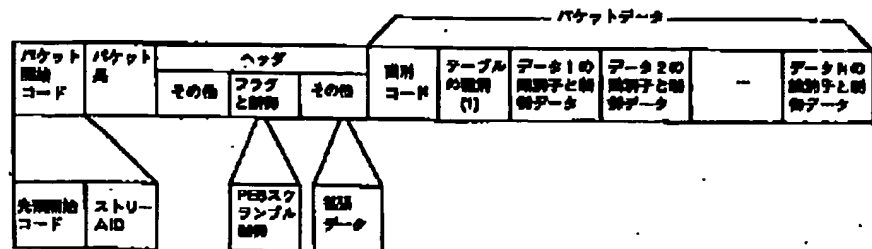


【圖 13】

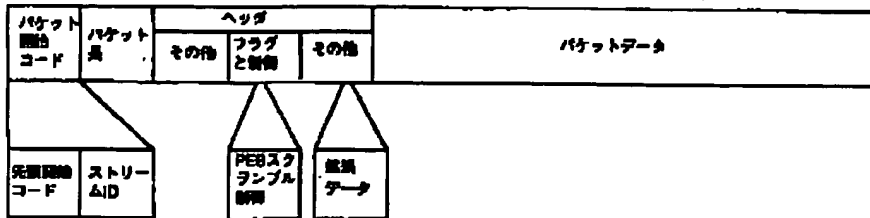
第2の診断テーブル



【圖 12】



【図14】



【図15】



【図16】

第1の制御テーブル	グループ識別子	制御データ (利用許可(1)/不可(0))
グループ1 (映像1 & 音声1)	1111 0001	1
グループ2 (映像2 & 音声2)	1111 0010	0
グループ3 (映像3 & 音声3)	1111 0011	0

第2の制御テーブル	識別子	制御データ (利用許可(1)/不可(0))
グループ1 (映像1 & 音声1)	1111 0001	1
グループ2 (映像2 & 音声2)	1111 0010	1
グループ3 (映像3 & 音声3)	1111 0011	0

【図17】

第1の制御テーブル	グループ識別子	データ識別子	制御データ (利用許可(1)/不可(0))
グループ1 (映像1 & 音声1)	1111 0001	1110 0001	1
グループ2 (映像2 & 音声2)	1111 0010	1110 0010	0
グループ3 (映像3 & 音声3)	1111 0011	1110 0011	0

※は0または1

第2の制御テーブル	グループ識別子	制御データ (利用許可(1)/不可(0))
グループ1 (映像1 & 音声1)	1111 0001	1
グループ2 (映像2 & 音声2)	1111 0010	1
グループ3 (映像3 & 音声3)	1111 0011	0

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.